Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Space Control and Information Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Space & Missile Defense Command,Army Forces Strategic Command,Redstone Arsenal,AL,35809**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**3**	

Space Control and Information Operations

By Jeff Harley

There exists today a symbiotic relationship between Space Control and Information Operations. Recent events in Operation Enduring Freedom show we are just now beginning to understand the mutual advantages these two communities provide.

The overarching focus of Joint Vision 2020 is full spectrum dominance achieved by the interdependent application of dominant maneuver, precision engagement, focused logistics and full dimensional protection. Information superiority becomes the key enabler to achieving full spectrum dominance — Information Operations (IO) and Space control have become the pillars. Army Space Operations Officers today need to understand the relationship between IO and Space control, and how Space control can support current and future information operations.

IO in a Nutshell

Information Operations do not merely attack computers, satellites, and communications networks. While IO may use these means to influence a decision-maker, IO considers how humans think and make decisions. IO also has to defend friendly information systems, decision-support systems, and decision-making. Ultimately, IO is about will. IO provides the U.S. the ability to influence an adversary's will to fight while protecting our forces and our will.

The Department of Defense Directive 3600.1 will define IO as "actions taken to influence, affect, or defend information, information systems, and decision making." DoD policy employs IO in support of full spectrum dominance by taking advantage of information technology, exploiting the growing worldwide dependence upon automated information systems, and capitalizing on near real-time global dissemination of information to affect an adversary's decision cycle with the goal of achieving information superiority for the United States.

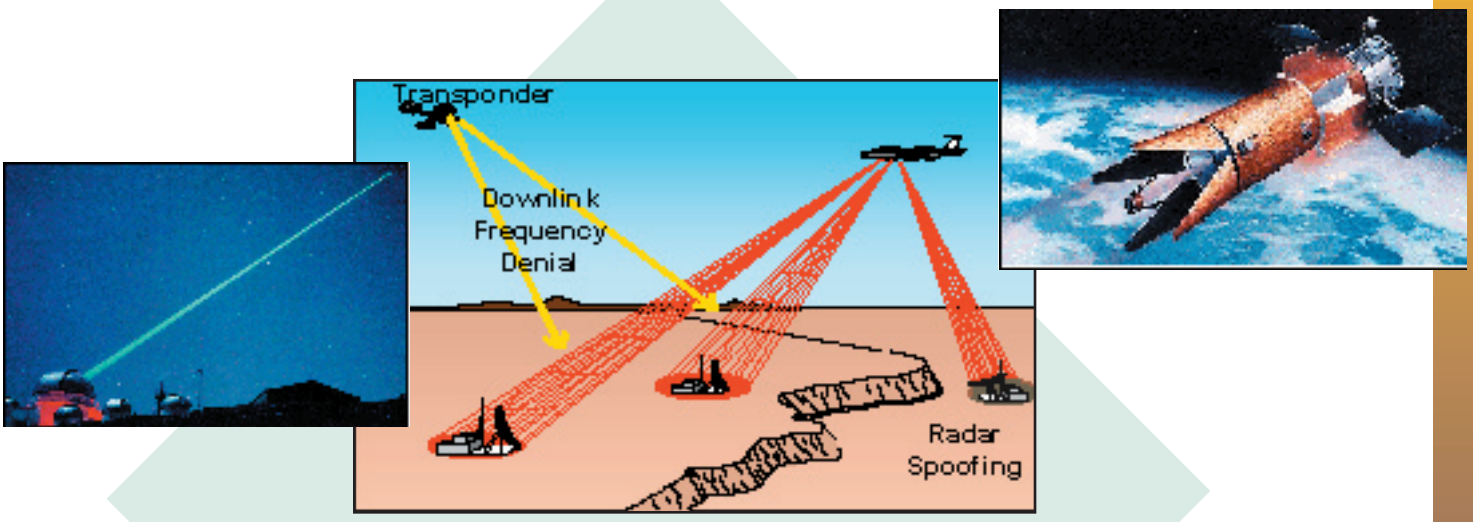
The new directive identifies only five core capabilities for IO. Psychological operations, military deception, and operations security capabilities influence the foreign decision-makers or groups and protect friendly decision-making. Computer Network Operations and Electronic Warfare capabilities affect or defend the electromagnetic spectrum, information systems, and information that support decision-makers, weapon systems, command and control, and automated responses. Computer Network Defense and Computer Network Attack comprise Computer Network Operations.

Counterintelligence, physical (i.e., kinetic) attack, physical security, and information assurance become IO supporting capabilities. These supporting capabilities can influence decision-makers or groups or target information systems, while detecting, safeguarding, and mitigating threats to our own information systems and decision-making processes. Public Affairs and Civil-Military Operations remain related IO capabilities, and help shape the information environment.

A misconception, or "urban myth," seems to have arisen in the last few years. All Space Operations Officers must understand that Space control is not an IO capability. They are two distinct mission areas governed by two separate sets of directives and manned by two unique force structures.

Space Control in a Nutshell

Today our military operations depend on Space capabilities. In the future, new doctrine, technologies, and force transformations will dictate an ever increasing reliance on Space services for command and control, communications, intelligence, navigation, and so forth. The protection of our Space capabilities and denial of an adversary's use of Space is key to information superiority. Lessons learned during the Desert Storm, Kosovo, and Operation Enduring Freedom campaigns underscore and demonstrate the value of operating in Space. Potential adversaries and unfriendly powers have noticed these lessons as well. Adversaries will probe



our Space systems for vulnerabilities. They may gain access to our systems and tamper with or exploit the data and information they carry. The assumption Space capabilities will always be there is wrong — there are no guarantees.

Space control provides "… freedom of action for friendly forces in Space while, when directed, denying it to an enemy," and consists of four operational elements. Space protection employs active and passive defensive measures to ensure U.S. and friendly Space systems operate as planned. Space surveillance monitors, detects, identifies, tracks, assesses, and categorizes objects in Space. Space prevention employs measures to prevent enemies' use of data or services from U.S. or friendly Space assets. Space negation denies freedom of action in Space to enemy forces by disrupting, denying, degrading, deceiving, or destroying enemy Space capabilities.

Space Control Support to IO

The ability to delay or deny information from Space systems, at any level of conflict, provides the basis for information dominance. The Army must seek control over the information or products Space systems provide; recognizing these Space systems are distributed weapon systems, consisting of three segments: an orbital segment, a ground segment, and a link segment. Attacking any of these three segments can provide information superiority and interrupt or affect an enemy's decision-making cycle without necessarily involving the physical destruction of systems or facilities.

Operational centers of gravity in the orbital segment of an enemy's Space system can be the entire satellite or the satellite subsystems critical for mission performance. We do not have to destroy a satellite to prevent it from accomplishing its mission and deny an adversary use of the Space environment. Temporarily damaging or disrupting vital satellite subsystems can prevent satellites from effectively accomplishing their mission. Examples of vital subsystems include satellite attitude control sensors, mission sensors, uplink/downlink antennas, and power generation systems. Directed at an orbiting satellite, high-energy beams projected into Space can dazzle or blind a satellite's sensors or cameras, interrupting or denying the flow of information at critical times.

The center of gravity in the link segment is the communications link, the radio frequency used to pass information to and from the satellite. Since most satellites rely on uplinked command and control information from the ground for station keeping, payload management, and satellite health and status functions, attacking a satellite's uplink during critical commanding periods could seriously degrade mission performance. The effectiveness of electronic jamming, however, is limited because of line of sight restrictions and increased satellite autonomy, therefore, attacking the downlink, rather than the uplink, is usually an easier and more reliable method of disrupting a Space system. Using Computer Network Attack or electronic warfare to attack the link segments provides the military a non-kinetic option to deny information to an adversary.

Since satellite downlink telemetry contains the mission information and health and status information on the Spacecraft and the satellite's sensor, successfully attacking the downlink directly attacks information flow and, therefore, may have a more immediate effect on achieving information dominance. Many countries, including Russia, China, Iraq, North Korea, Iran and Cuba, possess electronic jamming capabilities to disrupt satellite operations. Russia's Aviaconversia marketed a 4-watt Global Positioning System (GPS) jammer weighing about 19 pounds but capable of denying GPS reception for about 125 miles. Disrupting GPS signals can inhibit force-tracking systems, and influence military decision-makers.

The centers of gravity in the ground segment include satellite launch facilities, command and control facilities,

(See Information Operations, page 38)

and processing stations (airborne, sea-based, fixed or mobile land-based). All parts of the ground segment are vulnerable to attack from various means such as clandestine operations, air attack, direct ground attack, and IO.

Space Operations Officers bring their Space control expertise to IO. The latest Army IO field manual, FM 3-13, clearly establishes the Space Operations Officer as a member of the command's IO cell, and identifies some specific duties, such as:

- Including IO requirements in the Space operations appendix of the operations annex.
- Coordinating IO requirements with U.S. Army Space Command.
- Coordinating with IO targeting to include adversary Space system elements in the targeting process.
- Supporting operations security and military deception efforts by maintaining adversary Space order of battle, to include monitoring orbital paths and satellite coverage areas.
- Conducting operational planning analysis and determining how Space operations can meet IO requirements.

It is not a one-way street. As mentioned above, the relationship between Space control and IO is symbiotic — two unlike, yet closely associated mission areas providing each other mutual advantages. Space Operations Officers should also incorporate IO capabilities into their Space planning and operations. Computer Network Defense, physical security, counterintelligence, and information assurance capabilities can become part of Space protection planning. Computer Network Attack, electronic warfare and military deception can become Space negation options.

Integrating Space and Information Operations provides increased operational flexibility by increasing options available at any level of conflict. A Space Operations Officer who understands the basics of IO, and can contribute to the planning efforts, becomes more valuable to a commander than one who does not. These two mission areas will continue to expand and grow in importance, and enable the realization of Joint Vision 2020 - Full Spectrum Dominance.

Jeff Harley supports the U.S. Army Space Command, G-3 Plans, Information Operations Section in Colorado Springs, Colorado. He retired from the Army in 2000 after serving in numerous command and staff positions in the continental United States and Germany; including Department of the Army Inspector General, 104th Military Intelligence Battalion S-3, and Commander, A Company, 204th Military Intelligence Battalion.

Endnotes

1. DOD Directive 3600.1, Information Operations, is in final coordination and the Deputy Secretary of Defense should sign it before the end of Summer 2002.
2. Joint Publication 1-02, Dictionary of Military and Associated Terms, as amended through 15 October 2001.
3. Lt Col Robert H. Zielinski, et al, "Star Tek-Exploiting the Final Frontier: CounterSpace Operations in 2025," A Research Paper Presented to Air Force 2025, August 1996 (http://www.au.af.mil/au/2025/volume3/chap09/v3c9-1.htm#Introduction)
4. Jonathon Broder, "The Threat over the Horizon," MSNBC, undated (http://www.msnbc.com/news/561893.asp)
5. FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures, is in the final stages of approval, and replaces FM 100-6.